**IN RE: OFFICE WAREHOUSE INC.** **NPC BN 18-144**

x----------x

# RESOLUTION

**AGUIRRE, *D.P.C.;***

Before the Commission is a breach notification submitted by Office Warehouse, Inc. (OWI) involving the inadvertent disclosure of email addresses of its CLP Points Plus+ Cardholders.

## Facts

On 02 August 2018, OWI notified the National Privacy Commission (NPC) of a breach:

> This is to report a data breach involving approximately 1,900 email addresses of customers of Office Warehouse, Inc. (the "Company.")
>
> The incident happened when one of the staff of the Company unintentionally sent an email message to its customers without hiding, thus, exposing the email address of a certain customers to more or less 50 other customers. The delivery of email message was made per batch to at least 50 email users. The management was informed of the incident on July 30, 2018 at about 7:30 pm. The personal information involved in the incident are only email addresses.
>
> We are conducting further investigation on this incident and we will inform the Commission of the results thereof[.][1]

On 26 October 2020, the NPC, through its Complaints and Investigation Division (CID), issued an Order directing OWI to submit a Full Report within fifteen (15) days from receipt.[2]

---

[1] Personal Data Breach Notification from Office Warehouse, Inc., 02 August 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2018).
[2] Order, 26 October 2020, at 1-2, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).

On 13 November 2020, OWI submitted its compliance[3] and a copy of the emails that exposed its customers' email addresses.[4]

OWI reiterated substantially the same narration it provided in its initial notification. On 27 July 2018, OWI sent a marketing email to approximately one thousand nine hundred (1,900) customers' email addresses to remind them of the "Office Warehouse CLP Privacy Policy."[5] The emails were sent to CLP Points Plus+ Cardholders in thirty-seven (37) batches.[6] OWI's staff, however, claimed that it "unintentionally" sent the emails without using the blind carbon copy (BCC) function and exposed the email addresses of at least fifty (50) cardholders to other recipients of the same email.[7]

OWI stated that the email content did not involve information "that may lead to the identification of its members."[8] OWI added that "[t]he event was caused by a [sic] human error by one of [its] staff and [OWI] sent an apology letter to those recipients who responded via [] and [] email."[9]

On measures implemented to address the breach, OWI reported that it sent an apology letter to those recipients who responded to their marketing email.[10] OWI also stated that it reported and discussed the breach incident with its Data Protection Officer (DPO) and the OWI management.[11]

OWI also reported that it recalled all the emails sent without using the BCC function on 30 July 2018.[12] It identified that some of the emails were not successfully sent because (1) the email bounced back (Mailer Daemon), as the email inbox is full, the email address does not exist, or the email server is unavailable;[13] (2) the email was blocked by

---

[3] Data Breach Report Form, 13 November 2020, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[4] Data Breach Report Form, 13 November 2020, Email List_CLP Jul 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[5] *Id.* at 1.
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] Data Breach Report Form, 13 November 2020, at 2, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[11] *Id.*
[12] *Id.*
[13] *Id.*

Google, Yahoo and Global spam filters;[14] or (3) the email was deleted on the server due to queue status.[15] Thus, it reviewed emails in the deferred queue of Office Warehouse's server, checked "Global spam filters" of Gmail, Yahoo, and other mail addresses, and identified the number of active email addresses to whom the email was successfully sent.[16] Finally, OWI reported it "[r]eplied to the affected email recipient[s] to get updates on the action taken."[17]

On 24 September 2021, the CID directed OWI to submit additional information on the actions it reported to have been taken within five (5) days from receipt of the directive.[18] Specifically, the CID required the following:

1. A Full Investigation Report containing a description on the breach, its discovery, and root causes;[19]
2. Details of the incident response team's actions and decisions, specifically if certain emails were deleted, proof of deletion, if any, and the rationale behind such actions;[20]
3. The outcomes of breach management and any difficulties, including: the status of the recalled emails, review of emails in the deferred queue of OWI's server, check on global spam filters, identification of active email addresses involved, and updates provided to the affected email recipients;[21]
4. Compliance with notification requirements, including clarification on the number of affected data subjects, copies of the notification sent, proof of notification, copies of the apology letter to those recipients who responded to the original email, and proof of assistance provided to the data subjects;[22] and
5. Measures implemented post-incident to prevent future breaches, including updates to policies, employee training, and proof of these actions.[23]

On 22 October 2021, OWI submitted its compliance with supporting documents.[24]

---

[14] *Id.*
[15] *Id.*
[16] Data Breach Report Form, 13 November 2020, at 2, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[17] *Id.*
[18] Complaints and Investigation Division Email, 13 November 2020, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] Compliance, 22 October 2021, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).

OWI re-submitted its Data Breach Report Form dated 13 November 2020 to comply with the CID's directive to submit a Full Investigation Report.[25] OWI also stated that its Information Technology (IT) Team worked with its Marketing Staff "for email callback to reduce the bulk email sending that has been successfully done."[26]

OWI also submitted a breakdown of the number of recipients per email batch,[27] a copy of one of the emails sent without using the BCC function,[28] and a copy of the apology emails sent to the four (4) recipients who called out the incident.[29]

In response to one of the customers who emailed to point out OWI's failure to use the BCC function, OWI stated:

> Hello [OWI customer],
>
> Office Warehouse data privacy team, values your privacy and deeply regrets that this incident occurred. Our team has taken immediate actions to address your concern. Rest assured that the security and privacy of your personal data is of an utmost important to us and we are continually improving our systems and business processes to better serve you.
>
> Thank you for your understanding.
>
> Sincerely,
> Data Privacy Team
> Office Warehouse, Inc.[30]

OWI sent a similar response to the three (3) other recipients who pointed out the incident.[31] OWI assured them that it took immediate actions to address the incident and offered assistance for any other concerns.[32]

---

[25] *Id.* Annex 1.
[26] *Id.*
[27] *Id.* Annex 2.
[28] *Id.* Annex 3
[29] *Id.* Annex 4-5.
[30] Compliance, 22 October 2021, Annex 4, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[31] *Id.* Annex 5.
[32] *Id.*

OWI also explained in its compliance that it merely stated that it sent an apology to its data subjects and claimed the data subjects did not request further help.[33]

OWI submitted copies of the following: an internal memorandum reminding its employees on Email Policy and Etiquette (with translations in both English and Filipino),[34] its Privacy Awareness training material,[35] and its Email Etiquette Training slides presented during a Data Privacy Orientation conducted in 2018 for employees.[36]

On 25 January 2022, OWI resubmitted its compliance dated 22 October 2021.[37]

## Issue

Whether OWI sufficiently addressed the breach and implemented security measures to prevent its recurrence.

## Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Management). Nevertheless, OWI sufficiently addressed the breach and implemented security measures to prevent its recurrence.

Section 11 of NPC Circular 16-03 on mandatory breach notification provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include,

[33] Compliance, 22 October 2021, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[34] *Id.* Annex 6.
[35] *Id.* Annex 7.
[36] *Id.* Annex 8.
[37] Email Re: NPCBN 18-144, 25 January 2022, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2022).

but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

B. There is reason to believe that the information may have been acquired by an unauthorized person; and
C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[38]

Following this, the requisites for mandatory breach notification to the Commission are:

1. The breach involves sensitive personal information, or information that may, under the circumstances, be used to enable identity fraud;[39]
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[40]

The first requisite is absent in this case. The nature of the information involved is neither sensitive personal information nor other information that, under the circumstances, may enable identity fraud.

The first requisite of mandatory breach notification under Section 11 of NPC Circular 16-03 should be read together with Section 20 (f) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA). Section 20 (f) expressly requires the consideration of the specific circumstances of a breach in determining whether other information involved in the breach may enable identity fraud:

> Section 20. *Security of Personal Information.*
>
> . . .

[38] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[39] NPC BN 18-158, 13 November 2023, at 10 (NPC 2023) (unreported).
[40] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a Sua Sponte NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2024).

> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.[41]

The Commission previously held that a data subject's name and email may be considered under other information that may enable identity fraud.[42] The Commission explained:

> This Commission takes this opportunity to stress that information that may be used to enable identity fraud under Section 11 (A) is not limited to the categories of information listed therein, such as data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> **Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of "Phishing" attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.**[43]

In that case, the Commission, after considering the circumstances, determined that the names and email addresses of the data subjects are information that may be used to enable identity fraud.[44] The PIC

---

[41] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (f) (2012). Emphasis supplied.
[42] NPC BN 20-124, 10 September 2020, at 3 (NPC 2020) (unreported).
[43] *Id.* Emphasis supplied.
[44] *Id.* at 4.

reported that a hacker accessed and implanted ransomware in an online database.[45] Because of these particular circumstances, the Commission concluded that the hacker may contact and send malicious emails directly to the data subjects.[46]

Here, however, the inadvertent disclosure of the CLP Points Plus+ Cardholders' email addresses would not have enabled identity fraud.

In its initial report, OWI stated that "the personal information involved in the incident are only email addresses."[47] Later, in its compliance dated 13 November 2020, OWI reiterated that the email content did not involve information "that may lead to the identification of its members,"[48] and that the disclosed information was limited to email addresses only.[49] As proof, it also submitted a copy of the emails that exposed its customers' email addresses.[50]

OWI also explained in its submissions that the incident was "[c]aused by a [sic] human error by one of [its] staff"[51] when they "unintentionally" sent the emails without using the BCC function.[52]

Given the specific circumstances of this case, email addresses alone do not provide adequate means of committing identity fraud. As such, the email addresses of the data subjects cannot be considered as other information that may enable identity fraud.

The second requisite is present in this case. There was acquisition of the information by an unauthorized person.

The Commission previously held that a loss of control over personal data held in custody is enough for a personal information controller (PIC) to have "reason to believe that the information may have been acquired by an unauthorized person."[53]

---

[45] *Id.*
[46] *Id.*
[47] Personal Data Breach Notification from Office Warehouse, Inc., 02 August 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2018).
[48] Data Breach Report Form, 13 November 2020, at 1, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[49] *Id.*
[50] Data Breach Report Form, 13 November 2020, Email List_CLP Jul 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[51] *Id.* at 1.
[52] *Id.*
[53] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

In this case, OWI admitted that the marketing email was sent to thirty-seven (37) batches of CLP Points Plus+ Cardholders at a time without using the BCC function,[54] which made the other recipients' email addresses visible. Further, OWI submitted a copy of the apology emails sent to the four (4) recipients who responded to the email to point out the incident.[55] The foregoing shows that there is not just a reasonable belief but certainty that an unauthorized person acquired the information involved in the breach.[56]

The third requisite is also absent. There is no real risk of serious harm in this case.

The Commission takes this opportunity to discuss the factors considered in determining the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> . . .
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[57]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.[58] The risk must be apparent and not the product of mere speculation.[59] Serious harm

---

[54] Data Breach Report Form, 13 November 2020, at 1, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[55] Compliance, 22 October 2021, Annex 4-5, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[56] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[57] NPC Circ. No. 16-03, § 11.
[58] In re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8, available at https://privacy.gov.ph/wp-content/uploads/2024/06/NPC-BN-17-028-_-18-180-2023.05.11-Resolution-FinalP.pdf (last accessed 30 March 2024).
[59] *Id.*

means that the consequences and effects to any affected data subject are significant based on the surrounding circumstances of the breach.[60]

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.[61]

In this case, the objective of the unauthorized acquisition was not for some malicious or fraudulent purpose. As previously established, the disclosure of the email addresses was due to the OWI staff's inadvertent failure to use the BCC function.[62] Further, the nature and amount of information involved was limited to the email addresses of CLP Points Plus+ Cardholders.[63] This limited information did not provide the recipients with access to other details that would enable identity fraud. Thus, further exposure or misuse of the information is unlikely.

Finally, OWI implemented sufficient security measures to address the breach and prevent its recurrence. It recalled all the emails sent without using the BCC function on 30 July 2018.[64] OWI also sent apology emails to the four (4) recipients who called out the incident[65] and offered assistance for any other concern that may arise.[66] After the breach, OWI sent out an internal memorandum to remind employees on Email Policy and Etiquette.[67] It also conducted data privacy awareness training[68] and email etiquette[69] orientation for its employees.

---

[60] *Id.*
[61] *Id.*
[62] Data Breach Report Form, 13 November 2020, at 1, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[63] *Id.*
[64] *Id.* at 2.
[65] Compliance, 22 October 2021, Annex 4-5, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[66] *Id.* Annex 5.
[67] *Id.* Annex 6.
[68] *Id.* Annex 7.
[69] *Id.* Annex 8.

Given the foregoing factors and the remedial measures taken by OWI, the unauthorized acquisition did not give rise to a real risk of serious harm to any affected data subject. Thus, the third requisite is absent.

Considering that the first and third requisites are absent, the matter does not fall under mandatory breach notification. Nevertheless, OWI conducted proper breach management. The measures implemented by OWI are sufficient to address the breach and to prevent its recurrence.

**WHEREFORE,** premises considered, this Commission resolves that the matter of NPC BN 18-144 In re: Office Warehouse, Inc. is **CLOSED.**

**SO ORDERED.**

City of Pasay, Philippines.
21 March 2024.

**Sgd.**
**LEANDRO ANGELO Y. AGUIRRE**
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**
**JOHN HENRY D. NAGA**
Privacy Commissioner

**Sgd.**
**NERISSA N. DE JESUS**
Deputy Privacy Commissioner

Copy furnished:

**NRZ**
*Data Protection Officer*
**Office Warehouse, Inc.**

**COMPLAINTS AND INVESTIGATION DIVISION**
**ENFORCEMENT DIVISION**
**GENERAL RECORDS UNIT**
National Privacy Commission